Judge Marsha Pechman

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff, v. CHRISTOPHER MAXWELL, Defendant.	NO. CR06-42MJP GOVERNMENT'S SENTENCING MEMORANDUM

COMES NOW the United States of America, by and through John McKay, United States Attorney for the Western District of Washington, and Kathryn A. Warma, Assistant United States Attorney for said District, and files this Sentencing Memorandum.

I. Background and Status of the Case

Christopher Maxwell created, operated, and profited from a world-wide malicious botnet - an army of robot computers under his command - that he directed and controlled for at least 12 months from 2004 and into 2005. In January of 2005, Maxwell's botnet attacked the computer network of Northwest Hospital, in Seattle, Washington. Because the hospital quickly and courageously reported the attack to the FBI, agents were able to respond immediately and gather critical evidence, even while the attack was still in progress. With that evidence, dedicated agents from the FBI launched an exhaustive and complex investigation which, after six months of diligent and intensive pursuit, provided probable cause to obtain search warrants at the residence of Maxwell, in California, and two other co-conspirators, in Texas. Simultaneously, agents also executed seizure

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

warrants for the contents of six Paypal and bank accounts containing proceeds of the malicious botnet activity.

The Grand Jury for the Western District of Washington indicted Maxwell on February 9, 2006, on charges of Conspiracy, and Intentionally Causing and Attempting to Cause Damage to a Protected Computer. Maxwell pleaded guilty on May 4, 2006. The case is now before the Court for sentencing on August 25, 2006.

Due to the complexity and significance of this case; and due, as well, to disputed issues regarding sentencing factors, the United States will present evidence from the following witnesses during the sentencing hearing: 1) Special Agent David Farquhar, FBI; 2) Major Keithon Carponing, Joint Task Force - Global Network Operations, Department of Defense; 3) Gary Stine, CISSP, former Director of Information Technology, Colton, CA Unified School District; 4) Robert Steigmeyer, Vice President and CFO, Northwest Hospital; and 5) Gregory Schroedl, M.D., Vice President for Medicine and Chief Quality Officer, Northwest Hospital. With the exception of SA Farquhar, each of these witnesses is able to provide evidence on behalf of an organization that was victimized and suffered significant damage due to Maxwell's botnet. As such, they have a recognized right to be reasonably heard at sentencing pursuant to Title 18, United States Code, Section 3771(a)(4).

II. Statement of Facts

For at least one year, Christopher Maxwell willfully and persistently orchestrated a deliberate campaign of world-wide computer network attacks. Maxwell did so anonymously, from the private confines of his own home; secure, apparently, in the belief that the many steps he had taken to conceal his actions and identity would keep him forever above the law.

It is impossible to sentence Maxwell appropriately and reasonably without an understanding or appreciation of the extent of Maxwell's calculated and persistent criminal conduct and the magnitude of the damage he caused, as a result. And in order to

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

achieve that understanding, it is necessary first to consider at least a certain amount of technical information that pertains to both. Much of the technical information that is both critical and relevant in this regard was previously compiled and summarized in two documents prepared during the investigation of the Maxwell case. The United States respectfully refers the Court to those two important documents, and has appended them as Attachments A and B.

Attachment A is the affidavit of FBI SA David Farquhar, signed and sworn before the Honorable Kimberly Mueller, United States Magistrate Judge, on July 6, 2005. The affidavit was presented in support of a warrant approved by Judge Mueller for the search and seizure of computers and/or electronically stored evidence at the Maxwell residence.[1] This affidavit contains in as succinct a form as possible:

1) background information on the computer technologies used and exploited by Maxwell for his criminal botnet attacks (paragraphs 11 through 25), and 2) a chronicle of some of the important steps in the intensive six month search for the perpetrators of the NW Hospital botnet attack (paragraphs 27 through 90). All of that information is essential to an informed assessment of an appropriate sentence under the facts of this case. There are particular aspects, however, that warrant individualized emphasis because they evidence the attention, care, and effort Maxwell took to build, control, conceal, and profit from large scale criminal botnets over a twelve month period. Those aspects would include: the use of multiple IP addresses for resolution of the botnet sub-domain records - indicative of both intent and knowledge by Maxwell to create a "large scale, fault-tolerant system" (¶ 42); multiple hacks of organizational systems for use as illicit IRC servers (¶ 43); a history of over 200 connections to the DNS web site, to create, modify, and delete sub-domain records (¶ 44); use of a multitude of different e-mail addresses in course of criminal botnet conduct to conceal identity; (¶ 46); use of a compromised or stolen

[1]The affidavit is in redacted form to remove identifying information as to co-conspirators who were juveniles at the time the crimes were committed. See: 18 U.S.C. §5038.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

Netzero dial-up account to connect to the Internet for botnet purposes, which effectively concealed any connection from Maxwell's residence (¶ 49-54); data observed during the monitoring of Maxwell's IRC control server that would have revealed to Maxwell, (as it did to SA Farquhar), that during a single two week period in February of 2005, over 10,000 unique IP addresses were connecting to the botnet, indicating that over 10,000 computers/networks had been successfully hacked and victimized by Maxwell's botnet (¶ 57)[2]; receipt of over $30,000 in proceeds from multiple adware companies, which proceeds were generated by hacks and surreptitious installation of botnet code and adware on countless hacked computers/systems (¶ 64); collaboration with two co-conspirators purposefully to expand the scope of the botnet activity that included Maxwell's use of a debit card to fund a mobile phone account used by one of the juvenile co-conspirators (¶¶ 66-73, 80-87, 84).

While the July, 2005 affidavit (Attachment A) that was prepared for the limited purpose of obtaining a search warrant does thus provide a good deal of important information for purposes of assessing an appropriate sentence, it does not tell all. As the Maxwell case proceeded thereafter - through the charging phase, and even up to this date - further facts have continued to become known and associated with the case that are also significant and relevant to this end.

From the data that was captured during the two week period in February of 2005 in which Maxwell's botnet could be monitored, Agent Farquhar was able to identify some among the 441,000 victim computers/systems that had been hacked by Maxwell's botnet

---

[2]As noted infra, SA Farquhar's initial observation that Maxwell's botnet included "over 10,000" computers during the monitored two week period in February was offered only as a very preliminary estimate for purposes of establishing probable cause. After a subsequent thorough analysis that was made for the purpose of assessing accurately the number of victims, SA Farquhar concluded that Maxwell had control over at least 441,000 hacked "bot" computers during the two week time period of monitoring in February of 2005. Since this represented only 1/26 of the year long period during which Maxwell ran his botnet, and since Maxwell designed his particular botnet to perpetually "expand" in order to infect more machines to generate more profits through more adware installations, SA Farquhar has concluded and will testify at the hearing that Maxwell had hacked, and taken control over millions of computers during the twelve months that he continued to operate his botnet/s.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

during that relatively limited period of time. SA Farquhar made attempts as best he could, and as timely as he could, to contact those identifiable victims. One such apparent victim was the United States Department of Defense, signified by the fact that a ".mil" computer had been hacked and was reporting to Maxwell's botnet server. SA Farquhar therefore contacted the Department of Defense, which, in fact, had independently been pursuing its own investigation of persistent botnet attacks on military computers that had continued over a period of at least ten months launched by an actor that DOD had identified initially as "donttrip". The DOD investigation was conducted by the Joint Task Force - Global Network Operations (JTF-GNO). In February of 2006, the JTF-GNO issued an unclassified report in which they recounted their efforts to analyze and determine the source of botnet infections of DOD "hosts" (computers[3]) by "donttrip," who they had by then (due, in part, to collaboration with the FBI), determined to be Christopher Maxwell. That report, along with a data base that includes information on each DOD computer that was identified as compromised by Maxwell, constitutes Attachment B.

Again, the United States urges a complete and careful reading of that report as critical to a fully informed sentencing decision in this case. Among the contents of particular note in that report, is the "screen capture" of a website that Maxwell created and published on the Internet as "www.dontrip.org.". As noted in the JTF-GNO report, Maxwell, (hiding behind the screen name "donttrip"), "boasted"[4] from that website of payments he had received from various adware companies and urged visitors to his website to "click" on links he had provided in order that they, too, might "make money" in that same way.

---

[3]As will be explained by Mjr. Corpening, the hosts that Maxwell indiscriminately attacked ranged from desktop "pc's", to critical "servers" - which in turn had an impact on the scope of the consequence within the service component.

[4]Attachment B, at 10.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

The database appended to the Attachment B, JTF-GNO report is equally important, because it catalogues in detail the months and months of malicious infections[5] orchestrated by Maxwell, as well as their world-wide reach[6]. A review of the latter reveals, for example, that Maxwell's botnet/s infected and incapacitated computers at the Headquarters of the 5th Signal Command in Manheim, Germany; of the Directorate of Information in Fort Carson, Colorado; of the Navy Network Information Center in Pensacola, Florida; of the Navy Computer and Telecommunications Area Master Station, Central Europe, in Naples, Italy; of the DOD Bureau of Medicine and Surgery, in South Carolina; of the Headquarters of the Commander in Chief, U.S. Pacific Command, in Hawaii; of the Defense Investigative Service, in Maryland; of the U.S. Central Command at MacDill AFB, in Florida; and of the Health Care Systems Support Activity, in San Antonio, Texas, to name only a few.

The JTF-GNO report and supporting attack documentation concludes that Maxwell used his botnet/s to compromise a minimum of 407 DOD hosts; that a conservative estimate of the time it took, on average, to identify, rebuild, and reconfigures those infected machines was from three to five man hours each, resulting in a total loss of between 1,221 and 2,035 man hours. At an average man hour cost of $85.00 an hour, DOD estimated just a monetary loss to the DOD from "donttrip's" nefarious activities as between $103,785.00 and $172,975.00. DOD subsequently refined that loss figure to the specific amount of $138,000.00.; a loss figure that Maxwell did, in fact, acknowledge and agree, at the time of his plea, to pay as restitution.

Given the pressing demands of actively pursuing the NW Hospital investigation as Maxwell continuously "moved" the location of the bot command server, SA Farquhar made as many other attempts as time permitted to reach out to organizations, other than

---

[5] See: column 5, "start time," which was the date the attack was initiated.

[6] See: column 9, "DOD Description," which reflects the DOD component that was hit, and the geographic location of the infected host.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

DOD, which evidence indicated had been victimized by Maxwell's botnet. As SA Farquhar will testify, these communications were not always well received. In some cases, organizations were clearly resistant to requests to respond to or cooperate with the FBI, based on an apparent reluctance to be publically identified as the victim of a successful system hack. These experiences mirror the wide-spread recognition within the computer security industry that despite the billions of dollars in damages that have resulted from botnet attacks, "very few organizations step forward to identify themselves as victims . . . [because] [t]hey fear their reputation will be damaged for admitting to a bot infection."[7]

A third victim - beyond NW Hospital and DOD - that has been willing to come forward and publically acknowledge that they suffered devastating consequences from an attack by Maxwell's botnet is the Colton Unified School District, Colton, California. By letter of August 9, 2006, Superintendent Dennis Byas adopted by reference a letter transmitted electronically in June of 2005 by Gary Stine, CISSP, who was at that time Director of Information Technology at the Colton School District. That letter and a copy of the June 2005 communication are appended as Attachment C. In his June 2005 communication, Director Stine addressed both the substantial financial cost to this public school district, as well as the even greater educational loss to its students:

> We have a staff of 5 technicians who have spent approximately 70% of their time, on average, dealing with this virus threat since it proliferated throughout the District. Additionally, we have 2 technicians who have spent a significant amount of time troubleshooting and attempting to mitigate the virus threat at the server level. I estimate that the District has already lost approximately $50,000-$75,000 in labor costs alone due to this virus outbreak. However, there is a far greater cost that needs to be taken into consideration. The cost incurred from the loss of computers used by students and teachers for instructional purposes. We have had many computer labs of 36 or more computers taken down by this virus. The week or longer it takes to clean and repair the labs impacts the students who need

---

[7]Letter of Raymond Pompon, Information Security Manager, Network Computing Architects, 8/11/2006. Attachment F. See also: "Bringing Botnets Out of the Shadows," washingtonpost.com, section: "A Thankless Job". Article appended to Letter of Peter H. Gregory, CISA, CISSP, August 12, 2006.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

> this hardware for their educational endeavors. Setting aside the tremendous workload this virus has created for IT, the students, teachers, support staff and administrators of our District are the real victims. Instructional time lost can never be regained and is infinitely valuable.

Attachment C, page 2-3.

As noted above, former Director Gary Stine will offer testimony at the sentencing hearing, at which time he will provide additional detail regarding the calculation of financial loss to the Colton School District. Based upon a preponderance of evidence[8] on that issue, the United States will request that an order of restitution include those costs, in addition to those already agreed to by Maxwell in his Plea Agreement.

While it was readily apparent during the investigation that followed the NW Hospital intrusion that the botnet responsible was enormous, the focus of the investigation remained always on identifying, locating, and apprehending the perpetrator, and by this means to bring an end to what, up until day of apprehension, was continuing and clearly very dangerous criminal conduct. It was only more recently that a thorough analysis could be made by the FBI of the true scope of Maxwell's criminal botnet enterprise, for purposes of assessing sentencing consequences. The result of that analysis is a report prepared by SA David Farquhar, and appended as Attachment D.

The content of the Maxwell botnet analysis, like Attachments A and B, includes much that is technical in nature. It is, nonetheless, critically important and relevant information for determining the number of victims to Maxwell's crimes, which is, of course, a part of the sentencing process.

As demonstrated in SA Farquhar's report, and can further be explained by him during testimony, his analysis of data that was generated during only the very limited two week period in February of 2005, during which Maxwell's botnet was effectively monitored, indicates that approximately 441,558 unique IP addresses reported to

---

[8] 18 U.S.C. § 3664(e).

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

Maxwell's botserver. These IP addresses represent computers that were themselves infected and were actively infecting other computers, as evidenced by reports made to the botnet server by those computers. Of those 441,558 IP Addresses, 253,678 had useful reverse DNS entries that permitted further "per-domain" analysis. SA Farquhar refined and filtered this data to identify unique domains containing at least 10 unique IP addresses that were observed actively compromising other computers. Using this minimum number of 10 infected addresses per domain, SA Farquhar was able to identify 536 unique domain names with this level of infection. While individual IP addresses within the same domain might represent "double counting" of a single computer that is periodically assigned a new IP address, disparate domains likely represent different organizations, or at a minimum, different Internet Service Providers (ISPs) with different customers. As such, each domain represents either distinct victims, in the cases of non-ISP domains, or distinct ISPs, who have at least one, and more likely more than ten, victimized customers. The identities of those 536 victim domains are set forth at pages 11 through 14 of Attachment D. They include 104 country domains, 276 ".net" domains, 128 ".com" domains, and 28 ".edu" domains. As SA Farquhar will testify, each of these 536 victim domains (with a minimum of 10 unique infected addresses) very likely could have experienced a level of network damage that was similar in degree to that experienced by NW Hospital, the DOD, or the Colton Unified School District.

Another method exists, however, for reliably and conservatively computing the number of victims of Maxwell's criminal botnet activity. According to the information that Maxwell himself posted to his "donttrip" website[9], as well as information he provided to SA Farquhar during an interview, Maxwell was being paid for (surreptitious and unauthorized) adware installations at the rate of from one to 20 cents "per install."

[9]Attachment B, at 11.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

As SA Farquhar will testify, Maxwell also admitted during his interview that he was attempting to maximize his fraudulent revenues by effecting multiple "installs" on each infected bot machine. Assuming that Maxwell was able successfully to install as many as five different adware products on a machine that he successfully hacked, those multiple installs would yield commission payments to Maxwell that ranged from a total of five cents, to a maximum of one dollar, per machine infected.

PayPal records obtained during the investigation establish that Maxwell received over $32,000.00 in payments from adware companies during the period between June 2004 and April 2005.[10] Even assuming the highest possible rate of $1.00 per machine, these payments would evidence "successful" illegal hacks of and maximum adware installation on 32,000 computers. Assuming the rate of five cents per machine, the number would be 640,000 successfully infected machines. SA Farquhar will testify that even though it may not be reasonably possible to individually identify the owners of those thousands - or even millions - of damaged computers, it is reasonable to conclude that even in the case of a private, individual, "strictly recreational," "home PC" computer user, he or she would suffer pecuniary loss consequent to the infection of and damage to his/her computer from Maxwell's botnet[11]. A large percentage of victims, on the other hand, were likely sophisticated and networked institutions, like NW Hospital and DOD; which, even though they would be considered as only "one" victim, experienced damages and therefore losses in the range of $150,000. The United States submits that, given all of this evidence and using either of the above approaches for computing victim numbers, it would only be unreasonable not to conclude that the number of Maxwell's victims did not

---

[10] See Attachment E, Sworn Affidavit of SA Gabriel Gunderson, signed before Magistrate Judge Theiler, 7/6/2005, in support of seizure warrants for Maxwell's and co-conspirators' PayPal and bank accounts containing proceeds of criminal botnet intrusion - adware installation scheme.

[11] See, e.g., Letter of Lois Lehman, Attachment F, re: 5 hours needed to repair a bot infected computer, at a cost of $35.00 per hour = $175.00.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

exceed 250 in number. Finally, the United States appends as Attachment F letters from computer security professionals that have been written for submission to the Court in response to a request for input issued through Infragard, an organization sponsored by the FBI for vetted cyber security representatives from critical infrastructure organizations. The wealth of valuable information contained in these letters comes directly from experts in the IT security field, who have had very real and direct experience in combating botnets and the range of threats they pose.

As is noted repeatedly in those letters, botnets have in recent years become a preferred "M.O" for cyber criminal conduct that includes malicious distributed denial of service ("DDoS") attacks - many of these for extortion purposes; phishing schemes designed to steal credit and banking information; illegal spamming; theft of passwords and account numbers; porn and other illegal site-hosting; and also massive identity information theft through "sniffers" and key-loggers.[12] As of June, 2006, the cyber security organization CipherTrust offered a global bot count of 7,796,846.[13] Estimates of the financial damages that have been inflicted are no less staggering - running into the billions of dollars.[14] Of course, those estimates of financial costs (many of them to taxpayer funded institutions), take no account of indirect, "human" costs. The latter, as has been evidenced within this very case, can range from the lost educational opportunities cited by the Colton School District,[15] to impairment of military

---

[12]Letters, Russ McRee, HolisticInfoSec.org, at 2-3; Peter Gregory, supra, at 4,6.

[13]McRee Letter, supra, at 2.

[14]Pompon Letter, supra; see also: "2005 worst year for breaches of computer security," www.usatoday, 12/28/05 article appended to Peter Gregory letter.

[15]See also; Letter, Lois Lehman, in which this former Arizona State U. Computer Manager describes the non-financial costs to students, staff and faculty at ASU from a botnet attack. (Ms. Lehman also included an estimate of the financial cost of this attack at $35,000, based on need to restore 200 damaged computers, at 5 hours per computer, and a cost of $35.00 per hour for that work.)

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

communications on behalf of deployed U.S. military troops, to modifications and impairments in the provision of health care services as occurred in the wake of the NW Hospital attack. And as the malicious use of botnets continues to increase, so does the concomitant potential for even greater public harm - in the very plausible disruption, for example, of emergency response services, communications, public utilities, transportation services, banking, and agriculture. As stated by Peter Gregory, CISA, CISSP, to the Court, "A well-engineered botnet attack could throw a U.S. city, region, or industry sector into chaos for long periods of time, resulting in paralysis of vital services and loss of life."[16] Bots are appropriately analogized, he suggests, "as the automatic weapons of the Internet age, and bot*nets* as weapons of mass destruction."[17]

The genesis for this case was, in fact, a botnet attack that caused a wholesale disruption to the computer network of Seattle's NW Hospital, a 187 bed, community-based, not-for-profit hospital that relies daily on computers and the Internet to provide leading edge medical treatment that includes emergency, surgical, and intensive care services, as well as an array of diagnostic, laboratory, and outpatient care. As reflected in the Indictment, the consequences for the Hospital and its staff were profound - with impacts on the hospital's surgical system, information management system, diagnostic imaging services, and laboratory services. At the sentencing hearing, CFO Robert Steigmeyer will provide testimony regarding the chronology of the network attack, and describe the concerted, full-scale organizational response that followed over the course of the first critical days, and then weeks during which the NW staff restored the hospital's network and IT resources to pre-attack status. The financial cost of doing so, Mr. Steigmeyer will explain, totaled approximately $150,000.00.

---

[16]Gregory letter, supra, at 8.

[17]Gregory letter, id.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

Dr. Gregory Schroedl, Vice President for Medicine and an emergency room doctor, will provide testimony regarding the impact, and potential impact on patient clinical care at NW Hospital as a result of the attack. Both Mr. Steigmeyer and Dr. Schroedl will attest that although the potential for negative patient impacts as a result of a health care system network could be severe, NW Hospital's ongoing dedication to disaster preparedness, its long-term investment in technological resources, and its dedicated efforts to marshal all human resources necessary enabled the hospital continuously to provide its same high quality of care to its patients for the duration of the attack.

III. Argument

A. Proper Application of the Sentencing Guidelines Results in a Recommended Range of 70 - 87 Months Imprisonment

In the wake of United States v. Booker, 543 U.S. 220 (2005), the Sentencing Guidelines are no longer "mandatory." Still, the Supreme Court emphasized in Booker that the Guidelines did represent a form of "collective wisdom," and should be considered by the District Court as part of its sentencing deliberations:

> As we have said, the Sentencing Commission remains in place, writing Guidelines, collecting information about actual district court sentencing decisions, undertaking research, and revising the Guidelines accordingly. The district courts, while not bound to apply the Guidelines, must consult those Guidelines and take them into account when sentencing.

Booker, supra, at 264.

In keeping with the Supreme Court's directive, and its own independent belief that the Sentencing Guidelines do, indeed, represent the collective wisdom of informed experts who have particular insights and important global views on sentencing, the United States urges that the sentencing assessment in Maxwell's case properly should begin with an honest application, and computation under those Guidelines.

That computation would include the following:

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

Offense Level

Under U.S.S.G. §2B1.1:

(Offenses Involving Property Damage or Destruction, and Fraud and Deceit)

Base Offense Level:	6
Specific Offense Characteristics:	
Under U.S.S.G. §2B1.1(b)(1)(G):	
(Loss amount greater than $200,000[18])	+12
Under U.S.S.G. §2B1.1(b)(2)(A)©:	
(Offense Involved 250 or more victims)	+6
Under U.S.S.G. §2B1.1(b)(14)(iii):	
(Conviction under §1030 and disruption critical infrastructure)	+6
Adjusted Offense Level:	30
Adjustment for Acceptance of Responsibility	
U.S.S.G. §3E1.1(b):	-3
Total Offense Level, with Acceptance of Responsibility:	27

Criminal History

The government agrees that defendant has no criminal history, and therefore has a criminal history "Category" of "I."

Applicable Guideline Range

Based on an offense level of 27, and a criminal history category of I, the Guidelines yield a recommended range of imprisonment of from 70 to 87 months.

The United States believes that each of the referenced "specific offense category" adjustments are well supported in fact, and in law.

[18]As part of the Plea Agreement, the parties stipulated that the correct loss amount for purposes of sentencing was between $200,000.00 and $400,000.00. (Plea Agreement, paragraph 11.)

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

The first, of 12 points, is based on a loss amount in excess of $200,000. Application Note 3.(A)(v)(III) specifies that in § 1030 (intentional hacking) cases, "actual loss includes the following pecuniary harm, regardless of whether such pecuniary harm was reasonably foreseeable: any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other damages incurred because of interruption of service."

The United States believes that a full and accurate accounting of all of the losses that should be included under the terms of that definition would be difficult in this case. The Court, on the other hand, certainly is empowered to make such an assessment, which "need only . . . [be] a reasonable estimate of the loss," and properly could be made based, for example, on factors that include the "approximate number of victims multiplied by the average loss to each victim." Application Note 3.(c).

Based on the information that is available concerning the likely universe of millions of victims, the extent of the damage and the costs to repair that damage to just three identified victims, and information that has been provided by various experts on the minimum cost to repair a single bot-infected machine[19], a full loss figure doubtless would range in the tens of millions of dollars, or even higher.

At the time of the entry of plea, the United States was aware of the specific loss claimed by what were then two identified victims of Maxwell's botnet - NW Hospital and DOD. Combined, the losses suffered by just those two victims exceeded $200,000.00. Despite its belief that a loss figure of more than $200,000.00, (but less than $400,000) grossly underrepresents all of the losses that were inflicted by Maxwell during the year long period in which he hacked and damaged millions of computers, the United States

[19]See: ftnote 11.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

continues to honor the stipulation made as part of the Plea Agreement that the loss amount be recognized, for sentencing purposes, as falling at that low level.

The second adjustment, merely for "more than 250 victims", represents an equally gross under-assessment with respect to the true number of victims of Maxwell's attacks. As noted above, and will be reaffirmed in testimony of SA Farquhar, the number of computers (and computer owners) who suffered pecuniary damage and loss directly from Maxwell's intentional hacks and infections of their computers likely runs into the millions. The inability to attach a name to each individual computer owner should not prevent recognition of the reach and scope of Maxwell's willful and intentional criminal conduct. His crimes very literally extended world wide[20], and within only two weeks of their year long duration, infected - and thereby damaged - at least 441,000 computers.

The Sentencing Commission, as well as the courts, have consistently recognized that the scope of the criminal activity, as reflected by the number of victims, properly should be considered as a factor in computing an appropriate sentence. And in the "hacking conspiracy" context, in particular, the "over 250 victim" adjustment has been recognized as proper even in the absence of actual damage to more than 250 victims, when there is evidence that the defendant conspired to effect a hacking scheme to steal customer credit account numbers and he intended thereby to victimize at least 250 people who had such accounts. United States v. Salcedo, 2006 WL 1888816 (4th Cir. 7/10/06). Maxwell, too, was involved in just such a conspiracy - that had as its objective the persistent criminal hacking of as many computers as was possible, for a period of twelve months, in order to realize the maximum profit possible via the installation of adware on each such machine. And in Maxwell's case, unlike Salcedo, the hacker did achieve full success. Millions of machines were hacked and damaged in a way causing pecuniary loss, while Maxwell directly benefitted therefrom through the receipt of over $30,000 in criminal

[20]As evidenced by the country code domain names captured during monitoring.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

proceeds based on his voluminous hacks. An adjustment to Maxwell's Guideline computation based on "more than 250" victims is therefore proper and should be made.

The final six point adjustment for conviction under § 1030 and "substantial disruption of a critical infrastructure" is likewise proper and should be made. "Critical infrastructure" is defined within the Commentary to Guideline §2B1.1 at Application Note 13, as: ". . . systems and assets vital to national defense, national security, economic security, public health or safety, or any combination of those matters." (Emphasis added.) Maxwell's botnet attack devastated the network system of NW Hospital, a vital public health asset. Maxwell's botnet damaged and rendered inoperable 407 separate DOD computers - some of them servers - that were part of the systems of DOD components vital to national defense and security.

United States v. Mitra, 405 F.3d 492 (7th Cir. 2005), serves as an instructive case on this issue. The defendant Mitra had, in that case, hacked the computer-based radio system used by Madison, Wisconsin emergency responders. In summarily rejecting Mitra's argument that the critical infrastructure adjustment should not apply, the Seventh Circuit noted:

> [The] Application Note . . . defines [critical infrastructure]; Mitra concedes that an emergency radio system fits the definition. Emergency services are one of the note's examples. . . . . It is not as if the note were a linguistic garble, or that it is impossible to fathom why any sane person would think that the penalty for crippling an emergency-communication system on which lives depend should not be higher than the penalty for hacking into a web site to leave a rude message. The district judge was right to apply the guideline and note as written.

United States v. Mitra, supra, at 496-497.

Arguments could well be made that factors are present in Maxwell's case that would support additional upward enhancements or even an upward departure; including, for example, a minimum two point enhancement under § 3B1.1 for a leadership role within an organized conspiracy; a two point enhancement for the involvement and use of minors to commit a crime under §3B1.4, or upward adjustments based on the fact that the

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

loss amount and victim numbers used in the calculation are under-representative, in the extreme, of the true damage/loss amount and the number of people, institutions and organizations that Maxwell victimized. Alternatively, these or other factors referenced below could well support a request for a sentence at the high end of the computation outlined above.

With full consideration of these and other factors identified below, the United States urges the Court to make the Guideline computation as set forth above. Also for the reasons as explained more fully below, the United States asks that a sentence from within that range, of imprisonment for a term of 72 months, be imposed.

B. Factors Under § 3553(a) Support a Guideline Sentence of 72 Months Imprisonment, Which is Also a "Reasonable" Sentence

While the Sentencing Guidelines remain a starting point, post-Booker, the District Court must of course also consider the other factors identified in Title 18, United States Code, Section 3553(a), to reach a sentence that is "reasonable" taking all of those factors, as well as the Guidelines, into account. United States v. Carty, __ F.3d __, 2006 WL 1975895 (9th Cir. 7/17/06); United States v. Zavala, 443 F.3d 1165 (9th Cir. 2006). The "§ 3553(a) factors" include: the nature and circumstances of the offense; the history and characteristics of the defendant; the need for the sentence to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense; the need for the sentence to afford adequate deterrence to criminal conduct; the need for the sentence to protect the public from further crimes of the defendant; the need to provide the defendant with educational and vocational training, medical care, or other correctional treatment in the most effective manner; the kinds of sentences available; the need to provide restitution to victims; and the need to avoid unwarranted sentence disparity among defendants involved in similar conduct who have similar records.

Depending upon the facts and circumstances of a given case, certain of these factors assume greater or lesser import. The United States believes the following factors,

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

and considerations in relationship to them, support a sentence of 72 months of imprisonment for Christopher Maxwell.

The nature and circumstances of the offense.

The Guideline computation referenced above does not take into account the extended duration of Maxwell's criminal conduct - he persisted, relentlessly, in that conduct for no less than twelve months. Nor does the Guideline computation recognize the extraordinary level of effort, "dedication," and attention to detail that Maxwell must necessarily have devoted to building, constantly moving, concealing, rebuilding, and maintaining his massive, global botnet. SA Farquhar will provide evidence, at the sentencing hearing, of those extraordinary efforts as demonstrated repeatedly over the course of a year-long period.

All of those many efforts, it should also be emphasized, were devoted to earning profits for Maxwell, which necessarily involved damage and destruction to others. He only could make money if he was attacking, and damaging computers and networks of others. And, Maxwell collaborated with others, helping them to expand the reach of the criminal conduct (and its destructive consequences) beyond what he, alone, could achieve. Together, the three co-conspirators realized a combined total of $100,000.00 in proceeds from their hacks and illicit adware installations - a level of criminal proceeds and profits that have not otherwise been factored into the sentencing computation. Because a conspiracy did exist in this case, Maxwell is legally responsible for that larger loss, and his sentence should appropriately reflect that conspiracy-based liability. The "nature and circumstances" of the offense therefore weigh heavily in favor of a significant, 72 month term of imprisonment.

The need for the sentence to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense.

It is simply unbelievable that Maxwell could not have concluded, had he given it even just one minute of thought, that his botnet attacks would impact any and every kind of service, industry and institution throughout the world that was connected to the Internet

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

- and, that this would necessarily include health care providers, the United States military, and educational institutions, as well as emergency responders, utility services, transportation departments, and banking systems. An inability to forecast the identity of specific victims does not, and would not have magically "immunized" them from attack. Just as Maxwell hit a hospital and a school district - in the United States - with disastrous effects - he surely hit hospitals and school districts around the world. Not every hospital or school has the technological and human resources available to it as did NW Hospital, and the Colton School District. The potential that Maxwell created for world-wide system disasters - some of which may very well have cost lives - was real, and should absolutely be a consideration for this Court at sentencing.

Botnet crimes and the risks they pose to people and essential services around the world are deadly serious offenses that should be recognized as such, and sentenced accordingly.

The need for the sentence to afford adequate deterrence to criminal conduct.

The perpetrators of malicious botnets and those who use them for criminal ends are able to conceal their crimes and their identities in countless ways. Botnet cases are extremely difficult, time-consuming and labor intensive to investigate. Investigation and prosecution is hindered further by the reluctance of most organizational victims to report the crimes at the outset, or to agree to be publically identified as victims at any stage of the proceedings. There is, in addition, an unstated but perceptible resistance to the imposition of what is perceived as a "harsh" sentence for computer "hackers" who very often are relatively young, most often white, and largely from middle class backgrounds.

The "hacking"/botnet community is a true community, with their own publications, conferences, and avenues of communication. The need for serious sentences as an effective deterrent to hacking offenses is compelling, and if such a sentence is imposed in this case, it will be quickly communicated within the botnet community. A sentence that will not effectively deter, too, will be publicized - likely even more quickly.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

The kinds of sentences available and unwarranted sentence disparity.

A sentence of up to fifteen years imprisonment could possibly be ordered in this case. In the Mitra case (hack, by a graduate student, of the Madison, Wisconsin computer-based radio system), the district court imposed, and the Seventh Circuit affirmed, a sentence of 96 months imprisonment. United States v. Mitra, supra, at 493. In the Salcedo case (hack of Loew's network, in conspiracy to steal customer information), the district court ordered, and the Fourth Circuit affirmed, a sentence of 108 months imprisonment. United States v. Salcedo, supra, at 1888816. Certainly, there may be a variety of factors that are distinguishable and would warrant disparity between a sentence for Maxwell and these two other recent hackers.

Those distinctions, however, would likely work against Maxwell in terms of the duration of the conduct, number of victims, financial loss, and degree of harm caused. With all factors fairly considered, the government believes, a sentence of 72 months for Maxwell would not be so low as to create unwarranted disparities between these two other, similar recent hacking dispositions.

In sum, taking the Sentencing Guideline computation, as well as the pertinent factors of § 3553(a) into account, the United States submits that a sentence of imprisonment of 72 months would be proper, appropriate, and in this case fully reasonable.

C. The Judgment Should Include Restitution to NW Hospital, DOD, and the Colton Unified School District, as Well as Conditions Restricting Computer/Internet Access During Supervised Release

Maxwell has already agreed to restitution in the amount of $114,000.00 to NW Hospital, and $138,000.00 to the DOD. The United States intends to establish by both a preponderance, and "clear and convincing" evidence at the sentencing hearing that restitution should be ordered, as well to the Colton California Unified School District. An order to pay restitution to the school district should thus be included in the Judgment.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

The United States also asks that conditions of supervision include a prohibition on use of computers and access to the Internet, at any location (including employment) without the prior written approval of the Probation Office. Under the facts of this case, such a condition is reasonably related to the goal of deterrence, protection of the public, and rehabilitation of the offender, and involves no greater deprivation of liberty than is reasonably necessary for the purposes of supervised release. United States v. Rearden, 349 F.3d 608, 618 (9th Cir. 2003).

IV. Conclusion

On the grounds and for the reasons set forth above, the United States urges imposition of a sentence of 72 months imprisonment, followed by three years of supervised release, and an order of restitution to Northwest Hospital, the Department of Defense, and the Colton California Unified School District. Further, the United States seeks a preliminary order of forfeiture for a computer used in the criminal conduct, as well as funds that represent proceeds of the criminal conduct. Finally, the United States asks for conditions of supervision that would include restrictions, under Probation supervision, for computer and Internet access.

Dated this 18th day of August, 2006.

Respectfully Submitted,

JOHN McKAY
United States Attorney

/s/ Kathryn A. Warma
KATHRYN A. WARMA
Assistant United States Attorney
Washington Bar No. 12872
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
Telephone: (206) 553-8786
Fax: (206) 553-2502
E-mail: Kathryn.Warma@usdoj.gov

CERTIFICATE OF SERVICE

I hereby certify that on August 18, 2006 I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which will send notification of such filing to the attorney(s) of record for the defendant(s). I hereby certify that I have served the attorney(s) of record for the defendant(s) that are non CM/ECF participants via telefax.

s/ Jacqueline Masonic
JACQUELINE MASONIC
Supervisory Legal Assistant
United States Attorney's Office
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
Phone: (206) 553-4644
FAX: (206) 553-2502
E-mail: Jackie.Masonic@usdoj.gov